Claim 1:

The Examiner has rejected claim 1 under 35 U.S.C. §103(a) as unpatentable over Shwed et al. (WO 97/00471) in view of Lidinsky et al. (4,897,874). The Examiner states that it would have been obvious to include the step of determining that a data packet is being sent between members of a virtual private network in the method taught by Shwed.

Applicants have amended claim 1 to recite that the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, the secure data packet with an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units.

Applicants submit that the invention as claimed in claim 1 as amended, is neither taught, described, nor suggested in Shwed, or in Lidinsky, nor is there any suggestion to combine the references to result in the invention as claimed in claim 1.

The present invention provides an added measure of security by concealing the ultimate source and destination addresses in transit, by encapsulating the secure data packet, the secure data packet including an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units. (Specification, page 23, lines 5-10.) Thus, the data packet is not only modified through the various manipulation rules (described, for example, on page 6 of the Specification, lines 19-25): compression, encryption, and authentication, it is also encapsulated in another packet.

Although Shwed provides for some security by using a user generated rule base and modifying the data packet using decryption, signature verification, or address

verification, Shwed states that "[a]ll modifications are performed in accordance with the contents of the rule base." (Abstract) Thus, Shwed provides security through packet modification alone, without the additional step of encapsulation. As such, Shwed does not describe, teach, or suggest encapsulating the data packet in another packet to conceal the ultimate source and destination addresses in transit.

Moreover, Lidinsky discloses a high capacity metropolitan area network. The security features of Lidinsky's invention include "a port identification supplied by data concentrators, and a check that each packet is from an authorized source user, transmitting on a port associated with that user, to an authorized destination user that is in the same group as the source user." (Abstract.) As noted by the Examiner, Lidinsky discloses, as part of its security features, determining that the packet is being sent between members of the virtual network. Lidinsky does this determination, not by examining or modifying the data packet, but "by identifying the source port for each packet that is switched through the MAN network in order to ensure that only ports associated with a virtual network can access other ports of that network." (Column 3, lines 22-27)

Consequently, neither Shwed nor Lidinsky, alone or in combination, disclose the crucial security feature of packet encapsulation. The packets they deal with, un-encapsulated ones, are fundamentally different from the packets dealt with in the present invention – encapsulated ones.

Accordingly, the Applicants submit that claim 1 is patentable over any combination of Shwed and Lidinsky.

Claims 2-5:

Claims 2-5 are dependent on claim 1. As such, claims 2-5 are believed allowable for the same reasons as claim 1.

Claim 6:

The Examiner has rejected claim 6 under 35 U.S.C. §102(a) as anticipated by Shwed et al. (WO 97/00471).

Applicants have amended claim 6 to specify a method for recovering an original data packet from an encapsulated secure data packet sent between members of a virtual private network comprising the steps of ... de-encapsulating the encapsulated secure data packet.

As such, Applicants submit that claim 6 is not anticipated by Shwed et al. under 35 U.S.C. §102(a), as the two inventions are readily distinguishable.

The present invention provides for de-encapsulating the received secure data packet. (Specification, page 23, lines 17-25) This process reverses the encapsulation process which was used to conceal the ultimate source and destination addresses in transit. (Specification, page 23, lines 5-10)

Shwed, on the other hand provides for using a user generated rule base, and recovering the data packet using decryption, signature verification, or address verification according to the rule base. Indeed, Shwed states that "[a]ll modifications are performed in accordance with the contents of the rule base." (Abstract.) Thus, Shwed fails to teach either encapsulation or de-encapsulation as security features.

Accordingly, Applicants submit that claim 6 is not anticipated by Shwed et al. (WO 97/00471) under 35 U.S.C. §102(a).

Claims 7 and 8:

Claims 7 and 8 are dependent on claim 6. As such, claims 7 and 8 are believed allowable for the same reasons as claim 6.

Claim 9:

The Examiner has rejected claim 9 under 35 U.S.C. §102(a) as anticipated by Shwed et al. (WO 97/00471).

Applicants have amended claim 9 to include encapsulating the data packets, the data packets including address portions and data portions, entirely in encapsulating data packets which identify the source and destination addresses only for the virtual private network units.

As such, Applicants submit that claim 9 is not anticipated by Shwed et al. under 35 U.S.C. §102(a) as the two inventions are readily distinguishable.

The present invention provides for securing data packets by manipulating data traffic according to packet manipulation rules maintained by the first virtual private network unit, and by encapsulating the data packets, the data packets including address portions and data portions, entirely in encapsulating data packets which identify the source and destination addresses only for the virtual private network units. (Specification, page 23, lines 5-10)

Shwed, on the other hand provides for using a user generated rule base, and recovering the data packet using decryption, signature verification, or address verification according to the rule base. Indeed, Shwed states that "[a]ll modifications are performed in accordance with the contents of the rule base." (Abstract.) Thus, Shwed fails to teach the encapsulation of data packets as a security feature.

Accordingly, Applicants submit that claim 9 is not anticipated by Shwed et al. (WO 97/00471) under 35 U.S.C. §102(a).

Claim 10:

The Examiner objected to claim 10 "because of the following informality: In line 3, 'said first and second network addresses' should be 'said first and second computer [sic]'. Appropriate correction is required."

Applicants have amended claim 10 as indicated below.

10 (Amended). The system of claim 9 wherein said first and second virtual private network units include means for verifying that said first and second ~~network addresses~~ computers are both members of said virtual private network group.

Applicants have amended claim 10 as required, and request that the objection to claim 10 be removed.

Claim 11:

Applicants have amended claim 11 to more clearly define the present invention.

11 (Amended). The system of claim 10 wherein said first and second virtual private network units each ~~have~~ has an associated network ~~addresses~~ address, said network traffic utilizing the virtual private network addresses to conceal the identity of the first and second network addresses.

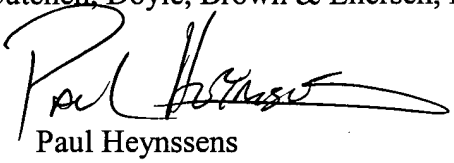
Claims 10 and 11, are dependent on claim 9. As such, claims 10 and 11 are believed allowable for the same reasons as claim 9.

The undersigned attorney welcomes comments and suggestions from the Examiner. If a telephone conversation can further prosecution of this case in any manner, the Examiner is urged to telephone the attorney at the number listed below.

Accordingly, in view of the above amendments and remarks it is submitted that the claims are patentably distinct over the prior art and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested. Based on the foregoing, Applicants respectfully request that pending claims 1-11 be allowed, and that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

McCutchen, Doyle, Brown & Enersen, LLP

By 

Paul Heynssens

Reg. No. 47, 648

Phone No. (213) 680-6880

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the claims:

Claim 1 has been amended as follows:

1 (Amended). A method for sending a first data packet from a first member of a virtual private network to a second member of said virtual private network comprising the steps of:

receiving said first data packet ~~enroute~~ en route to said second member;

determining that said first data packet is being sent between members of said virtual private network;

determining the packet manipulation rules for packets sent between members of said virtual private network;

forming a secure data packet by executing said packet manipulation rules on said first data packet; and

forwarding said secure data packet to said second member of said virtual private network,

wherein said secure data packet contains information of a source address and a destination address of said first data packet; and

wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, the secure data packet including an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units.

Claim 2 has been amended as follows:

2 (Amended). The method according to claim 1 wherein said step of determining that said first data packet is being sent between members of said virtual private network comprises the step of comparing the source and destination addresses of the first data packet to addresses stored in a virtual private network address table.

Claim 3 is unchanged.

Claim 4 has been amended as follows:

4 (Amended). The method according to claim 3 wherein said step of forming a secure data packet comprises the steps of:

encrypting at least a payload portion of the first data packet according to the identified encryption algorithm; and

providing authentication information for the first data packet according to the identified authentication algorithm.

Claim 5 has been amended as follows:

5 (Amended). The method according to claim 3 wherein said forming a secure data packet includes the step of concealing the source and destination addresses of the first data packet according to the identified packet manipulation rules.

Claim 6 has been amended as follows:

6 (Amended). A method for recovering an original data packet from ~~a~~ an encapsulated secure data packet sent between members of a virtual private network comprising the steps of:

receiving said encapsulated secure data packet;

de-encapsulating the encapsulated secure data packet;

determining the packet manipulation rules for packets sent between members of said virtual private network;

recovering the original data packet by manipulating the secure data packet by reversing the identified packet rules; and

forwarding the recovered original data packet to its destination,

wherein said original data packet contains information of a source address and a destination address of said secure data packet.

Claim 7 is unchanged.

Claim 8 is unchanged.

Claim 9 has been amended as follows:

9 (Amended). A system for securely exchanging data packets between members of a virtual private network group comprising:

a first computer at a first site, said first computer having a first network address;

a first router associated with said first site, for routing data packets originating from said first computer over the public network;

a first virtual private network unit disposed between said first router and said public network, said first virtual public unit for identifying virtual private network group data traffic and for securing said data traffic by manipulating said data traffic according to packet manipulation rules maintained by said first virtual private network unit, and by encapsulating the data packets, the data packets including address portions and data portions, entirely in encapsulating data packets which identify the source and destination addresses only for the virtual private network units;

a second router associated with a second site for coupling said second site to the public network;

a second virtual private network unit disposed between said second router and the public network for intercepting network traffic destined for said second site, said second virtual public network unit for detecting virtual private network group traffic and for recovering original packet data; and

a second computer at said second site, said second computer having a second network address for receiving said packet data,

wherein said data packet contains information of a source address and a destination address of said data packet.

Claim 10 has been amended as follows:

10 (Amended). The system of claim 9 wherein said first and second virtual private network units include means for verifying that said first and second ~~network addresses~~ computers are both members of said virtual private network group.

Claim 11 has been amended as follows:

11 (Amended). The system of claim 10 wherein said first and second virtual private network units each ~~have~~ has an associated network ~~addresses~~ address, said network traffic utilizing the virtual private network addresses to conceal the identity of the first and second network addresses.